IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

JANE C. ANGEL-LOPEZ, BARBARA J. LUJAN, ANTOINETTE MADRID, on behalf of themselves individually and all others similarly situated;

Plaintiffs,

v.

COMMUNITY HEALTH SYSTEMS, INC., a Delaware Corporation; COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION, a Delaware Corporation; SAN MIGUEL COUNTY HOSPITAL CORP., dba ALTA VISTA REG'L HOSPITAL; CARLSBAD MEDICAL CENTER LLC, dba Carlsbad Medical Center; ROSWELL HOSPITAL CORP., dba EASTERN NEW MEXICO MEDICAL CENTER; DEMING HOSPITAL CORP., dba MIMBRES MEMORIAL HOSPITAL; LAS CRUCES MEDICAL CENTER LLC, dba MOUNTAINVIEW REG'L MEDICAL CENTER; LEA REG'L MEDICAL CENTER LLC, dba LEA REG'L HOSPITAL; MILLS AVENUE MEDICAL CLINIC; and ALTA VISTA ORTHOPEDIC SPECIALISTS,

Defendants.

Case No. 14-CV-929 JB/CG
FIRST AMENDED COMPLAINT

CLASS ACTION COMPLAINT

COME NOW JANE C. ANGEL-LOPEZ, BARBARA J. LUJAN, and ANTOINETTE MADRID, on behalf of themselves individually and all others similarly situated, by and through their attorneys Branch Law Firm (Turner W. Branch, Margaret Moses Branch and Mary Lou Boelcke) and Slack & Davis LLP (Michael Slack and Paula Knippa), and bring this action against Defendants Community Health Systems, Inc.; Community Health Systems Professional Services Corporation; San Miguel County Hospital Corp.; Carlsbad Medical Center LLC; Roswell Hospital Corporation; Lea Regional Medical Center LLC; Las Cruces Medical Center LLC; Deming Hospital Corporation; Alta Vista Orthopedic Specialists; and Mills Avenue Medical Clinic, and allege as follows:

I. PARTIES

1. Plaintiff Jane C. Angel-Lopez, individually and as class representative, is a resident of San Miguel County, New Mexico, and a citizen of New Mexico. Jane C. Angel-Lopez treated at San Miguel County Hospital Corporation at all times material to this Complaint.

2. Plaintiff Barbara J. Lujan is resident of San Miguel County, New Mexico, and a citizen of New Mexico. Barbara J. Lujan treated at San Miguel County Hospital Corporation, Mills Avenue Medical Clinic, Ridge Runner Medical Clinic and Alta Vista Medical Clinic at all times material to this Complaint.

3. Plaintiff Antoinette Madrid is a resident of San Miguel County, New Mexico, and a citizen of New Mexico. Antoinette Madrid treated at San Miguel County Hospital Corporation at all times relevant to this Complaint.

4. Defendant Community Health Systems, Inc. ("CHS") is a Delaware corporation with its principal place of business in Tennessee. This Defendant, upon information and belief, does business in New Mexico, as well as 28 other states. CHS is the parent company that owns

and operates, through subsidiaries, 206 general acute care hospitals in 29 states with approximately 31,000 licensed beds. CHS is, or was at all relevant times, the parent company for the named hospital defendants.

5. Defendant Community Health Systems Professional Services Corporation ("CHSPSC") is a Delaware corporation with its principal place of business in Tennessee. Upon information and belief, CHSPSC does business in New Mexico as well as 28 other states.

6. Defendant San Miguel County Hospital Corporation, dba Alta Vista Regional Hospital, ("Alta Vista") is a New Mexico corporation with its principal place of business in Las Vegas, New Mexico. Alta Vista is, or was at all relevant times, a subsidiary of CHS and CHSPSC that operates a hospital in Las Vegas, New Mexico with 54 licensed beds.

7. Defendant Carlsbad Medical Center LLC, dba Carlsbad Medical Center, ("Carlsbad") is a New Mexico corporation with its principal place of business in Carlsbad, New Mexico. Carlsbad is, or was at all relevant times, a subsidiary of CHS and CHSPSC that operates a 115-bed facility with inpatient, outpatient, diagnostic, medical surgical and emergency services. It is an accredited Level III Trauma Center.

8. Defendant Roswell Hospital Corporation, dba Eastern New Mexico Medical Center Hospital, ("Eastern") is a New Mexico corporation with its principal place of business in Roswell, New Mexico. Eastern is, or was at all relevant times, a subsidiary of CHS and CHSPSC that operates a 162-bed facility with complete inpatient and outpatient care.

9. Defendant Deming Hospital Corporation, dba Mimbres Memorial Hospital, ("Mimbres") is a New Mexico corporation with its principal place of business in Deming, New Mexico. Mimbres is, or was at all relevant times, a subsidiary of CHS and CHSPSC that operates a 25-bed inpatient hospital.

10. Defendant Las Cruces Medical Center LLC, dba MountainView Regional Medical Center, ("MountainView") is a New Mexico corporation with its principal place of business in Las Cruces, New Mexico. MountainView is, or was at all relevant times, a subsidiary of CHS and CHSPSC that operates a 168-bed facility providing inpatient and outpatient care.

11. Defendant Lea Regional Medical Center LLC dba Lea Regional Hospital, ("Lea") is a New Mexico corporation with its principal place of business in Hobbs, New Mexico. Lea is, or was at all relevant times, a subsidiary of CHS and CHSPSC that operates a 201-bed acute care facility providing complete medical care.

II. JURISDICTION & VENUE

12. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act. 28 U.S.C. §1332(d)(2).

13. Venue is proper in this judicial district under 28 U.S.C. section 1391 because the Defendants do business throughout this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district. At all times material hereto, Defendants were and are in the business of providing services through general acute care hospitals and clinics in New Mexico, and in 28 other states, by and through various hospitals and clinics operated through subsidiary companies.

14. This court has personal jurisdiction over every named defendant in this matter.

III. SUMMARY OF CASE

15. This is a consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all other similarly situated persons ("Class Members"), whose personal information (e.g., patient names, addresses, birthdates, telephone numbers, and social security numbers and, possibly including, patient credit card, medical and/or clinical information) ("Sensitive

Information" or "PII/PHI") considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") entrusted to Defendants was stolen and/or made accessible to hackers and identity thieves.

16. As a result of Defendants' failure to implement and follow basic security procedures, Plaintiffs' Sensitive Information is now in the hands of thieves and being exploited. Plaintiffs named herein have experienced actual identity theft and are in imminent danger of ongoing and future identity theft because of Defendants' negligence. Consequently, Plaintiffs and the Class Members will have to spend significant time and money to remedy the problems created by this identity theft and to protect themselves from future exploitation.

17. Additionally, as a result of Defendants' failure to follow contractually-agreed upon, federally-prescribed, industry-standard security procedures, Plaintiffs received only a diminished value of the services they paid Defendants to provide. Plaintiffs contracted for services that included a guarantee by Defendants to safeguard their personal information and, instead, Plaintiffs received services devoid of these very important protections. Accordingly, Plaintiffs allege claims for breach of contract, unjust enrichment, money had and received, negligence, negligence per se, violation of the New Mexico Unfair Trade Practices Act, and breach of confidence.

IV. FACTS COMMON TO ALL COUNTS

18. Plaintiffs are patients and customers of Defendants' hospitals and clinics.

19. In the regular course of business, Defendants collect and maintain possession, custody, and control of a wide variety of Plaintiffs' Sensitive Information, including but not limited to patient credit card, medical or clinical information and history, patient names, addresses, birthdates, telephone numbers and social security numbers.

20. Plaintiffs and Defendants agreed that, as part of the services provided to Plaintiffs, Defendants would protect Plaintiffs' Sensitive Information.

21. This agreement to protect Plaintiffs' Sensitive Information was a value added to the services provided by Defendants that was considered a benefit of the bargain for which Plaintiffs paid adequate consideration.

22. Upon information and belief, a portion of the consideration paid by Plaintiffs and accepted by Defendants was to be allocated towards protecting and securing Sensitive Information and ensuring HIPAA compliance.

23. Defendants stored Plaintiffs' Sensitive Information in an unprotected, unguarded, unsecured, and/or otherwise unreasonably protected electronic and/or physical location.

24. Defendants did not adequately encrypt, if at all, Plaintiffs' Sensitive Information.

25. Defendants did not provide adequate security measures to protect Plaintiffs' Sensitive information.

26. On or around April 2014 and June 2014, an "Advanced Persistent Threat" group originating from China accessed, copied, and transferred Plaintiffs' Sensitive Information in the custody, care and control of Defendants.

27. The data accessed, copied, and transferred included Plaintiff's' Sensitive Information that is considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") because it includes patient names, addresses, birthdates, telephone numbers and social security numbers.

28. On or about August 18, 2014, CHS filed a Form 8-K with the United States Securities and Exchange Commission that provided the first notification of the data breach. This filing stated that the data breach "affected approximately 4.5 million individuals." This filing also stated that those affected were provided services by CHS within the last five years.

29. Defendants failed to take action to promptly notify Plaintiffs that were affected by the breach.

30. Defendants' failure to notify Plaintiffs of this data breach within a reasonable time caused Plaintiffs to remain ignorant of the breach and, therefore, unaware of the necessity of taking action to protect themselves from harm.

31. Defendants designed and implemented their policies and procedures regarding the security of protected health information and Sensitive Information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected health information and other Sensitive Information. Upon information and belief, Defendants failed to encrypt, or adequately encrypt, Plaintiffs' Sensitive Information.

32. As a result of Defendants' failure to implement and follow basic security procedures, the Sensitive Information of 4.5 million patients (including Plaintiffs and the class they seek to represent) is now in the hands of thieves. As a result of Defendants' failure to implement and follow basic security procedures, Plaintiffs suffered actual identity theft when unauthorized third-parties, on two occasions (in April and June 2014), accessed, transferred, and copied the Sensitive Information of 4.5 million patients.

33. The hackers deliberately targeted Defendants' computers and servers and spent several months collecting, accessing, and transferring Plaintiffs' Information. The hackers targets Plaintiffs' Sensitive Information for the sole purposes of misusing it.

34. Plaintiffs' identities were stolen, and they now face a substantial increased risk of additional instances of identity theft and resulting losses. Plaintiffs have suffered the theft of their identities and other injuries, and are immediately and imminently in danger of sustaining further direct injury/injuries as a result of the identity theft they suffered when Defendants did not protect and secure their Sensitive Information and disclosed it to hackers. These further

instances of identity theft are impending and imminent. Unlike other prominent data breaches, the Sensitive Information accessed, copied, and transferred has all of the information wrongdoers need, and the American government and financial system requires, to completely and absolutely misuse Plaintiffs' identity to their detriment.

35. Consequently, Defendants' patients and former patients have or will have to spend significant time and money to protect themselves; including, but not limited to: the cost of responding to the data breach, cost of conducting a damage assessment, costs of rehabilitate Plaintiffs' Sensitive Information, and costs to reimburse from losses incurred as a proximate result of the breach.

36. Additionally, as a result of Defendants' failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiffs received only a diminished value of the services they paid Defendants to provide.

37. Plaintiffs contracted for services that included a promise by Defendants to safeguard, protect, and not disclose their personal information and, instead, Plaintiffs received services devoid of these very important protections.

38. As a proximate result of Defendants' wrongful acts and omissions, Plaintiffs and the Class Members have suffered injury, harm, and damages including but not limited to the theft of their Personal Sensitive Information, emotional distress, loss of monies paid to Defendants for services to protect and not disclose Sensitive Information, and Plaintiffs and class members have and will have to spend significant time and money to protect themselves; including, but not limited to: the cost of responding to the data breach, cost of conducting a damage assessment, costs to obtain credit reports, costs to obtain future credit reports, cost for credit monitoring, costs for insurance to indemnify against misuse of identity, costs of rehabilitate Plaintiffs and class members' Sensitive Information, and costs to reimburse from losses incurred as a

proximate result of the breach.By failing to fulfill their promise to protect Plaintiffs' Sensitive Information, Defendants have deprived Plaintiffs of the benefit of the bargain. As a result, Defendants cannot equitably retain payment from Plaintiffs—part of which was intended to pay for the administrative costs of data security—because Defendants did not properly secure Plaintiffs' information and data. Under HIPAA and the HITECH Act, Defendants must implement policies and procedures to limit physical access to their electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. See 45 C.F.R. §164.310.

39. Specifically, Defendants must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmit; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted. See 45 C.F.R. §164.306.

40. Defendants must also implement technical policies and procedures for electronic information systems that maintain electronic SENSITIVE INFORMATION to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F. R. §164.308(a)(4).

41. A few of these policies and procedures include, but are not limited to: implementing a mechanism to encrypt and decrypt electronic SENSITIVE INFORMATION; implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic SENSITIVE INFORMATION; implementing procedures to verify that a person or entity seeking access to electronic SENSITIVE INFORMATION is the one claimed; implementing technical security measures to

guard against unauthorized access to electronic SENSITIVE INFORMATION that is being transmitted over an electronic communications network; implementing security measures to ensure that electronically transmitted electronic SENSITIVE INFORMATION is not improperly modified without detection until disposed of. See 45 C.F.R. §164.312.

42. When Defendants permit business associates to create, receive, maintain, or transmit electronic SENSITIVE INFORMATION, it must ensure that those business associates comply with HIPAA and the HITECH Act. See 45 C.F.R. §164.314.

43. Defendants must also conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate; implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and implement procedures for guarding against, detecting, and reporting malicious software. See 45 C.F.R. §164.308 (emphasis added).

44. Defendants did not comply with any of the foregoing requirements.

V. INDIVIDUAL FACTS

45. Jane Angel-Lopez was a patient at San Miguel County Hospital Corporation and Alta Vista Orthopedic Specialists for the past number of years, including December 2005, January 2006, December 2008, January 2009 and April 2014. Angel-Lopez provided personal and Sensitive Information to Defendants CHS, CHSPSC and San Miguel Hospital and Alta Vista Orthopedic Specialists on these dates. In August 2014, she received a letter from Alta Vista Orthopedic Specialists that that "some of your personal information may have been taken during the cyber-attack" on CHSPSC's computer network. After the cyber-attack, Ms. Angel-Lopez's Visa card was fraudulently used. Plaintiff believes the card information was obtained during the cyber-attack.

46. As an essential part of the services provided, Defendants CHS, CHSPSC and Alta Vista agreed to protect her personal and Sensitive Information.

47. Barbara J. Lujan was a patient at San Miguel County Hospital Corporation, Ridge Runner Medical Clinic and Mills Avenue Medical Clinic from March 2009 to the present. Lujan provided personal and Sensitive Information to Defendants CHS, CHSPSC, Ridge Runner Medical Clinic, Mills Avenue Medical Clinic, and San Miguel Regional Hospital Corporation on these dates. In August 2014, she received a letter from Mills Avenue Medical Clinic stating that "some of your personal information may have been taken during the cyber-attack" on CHSPSC's computer network. After the cyber-attack, Ms. Lujan received a call allegedly from the Internal Revenue Service ("IRS") demanding payment on owed taxes, although she did not owe any taxes to the IRS. Plaintiff believes this call was a result of her personal information being stolen during the cyber-attack.

48. As an essential part of the services provided, Defendants CHS, CHSPSC, Ridge Runner Medical Clinic, Mills Avenue Medical Clinic, and San Miguel Regional Hospital Corporation agreed to protect her personal and Sensitive Information.

49. Antoinette Madrid was a patient at San Miguel County Hospital Corporation in December 2011, February 2013 and January 2014. Madrid provided personal and Sensitive Information to Defendants CHS, CHSPSC, and San Miguel Regional Hospital Corporation on these dates. In October 2014, she received a letter from CHS and/or CHSPSC stating that "you have received or been referred for services from physicians at a clinic or hospital affiliated with Community Health Systems Professional Services Corporation." It also stated that "federal law enforcement authorities" sent a list to CHSPSC of individuals whose personal information was hacked during the cyber-attack and that list included Madrid. After the cyber-attack, Madrid's social security number, date of birth and other information were used without her approval.

Plaintiff believes this unapproved use of her personal information resulted from the theft of her personal information during the cyber-attack.

50. As an essential part of the services provided, Defendants CHS, CHSPSC, and San Miguel Regional Hospital Corporation agreed to protect her personal and Sensitive Information.

51. As a result of the data breach, all Plaintiffs have suffered emotional distress and economic harm, including but not limited to: loss of payment to Defendants—part of which was intended to pay for the administrative costs of data security—because Defendants did not properly secure Plaintiffs' personal and Sensitive Information, diminution in the value of services provided, emotional and/or mental distress as a result of identity theft, economic costs as a result of identity theft, and future expenses for credit monitoring.

VI. CLASS ALLEGATIONS

52. Plaintiffs bring this action pursuant to NMRA 1-023(b)(2) and (3) on behalf of themselves and Class and subclasses defined as follows:

53. **The Plaintiff Class**: Plaintiffs bring this action on behalf of themselves and a Class of similarly situated individuals, defined as follows:

All individuals in the United States who are current or former customers/patients of CHS and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months of April 2014 to June 2014.

54. In the alternative, Plaintiffs bring this action on behalf of themselves and a Class of similarly situated individuals, defined as follows:

All individuals in the State of [each individual State where CHS does business] who are current or former customers/patients of CHS and its affiliates and subsidiaries and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months of April 2014 to June 2014.

Plaintiff proposes the following subclasses in New Mexico:

a. **San Miguel County Regional Hospital Corporation**: All individuals in the United States who treated at San Miguel County Regional Hospital or its clinics and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months on or about April 2014 and June 2014.

b. **Carlsbad Medical Center LLC**: All individuals in the United States who treated at Carlsbad Medical Center LLC or its associated clinics and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months on or about April 2014 and June 2014.

c. **Roswell Hospital:**: All individuals in the United States who treated at Roswell Hospital Corporation (dba Eastern New Mexico Medical Center Hospital) or its associated clinics and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months on or about April 2014 and June 2014.

d. **Deming Hospital Corporation**: All individuals in the United States who treated at Deming Hospital Corporation or its associated clinics and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months on or about April 2014 and June 2014.

e. **Las Cruces Medical Center**: All individuals in the United States who treated at Las Cruces Medical Center LLC or its associated clinics and whose Sensitive Information was wrongfully accessed, copied, and transferred in the months on or about April 2014 and June 2014.

f. Lea Regional Medical Center LLC: All individuals in the United States who treated at Lea Regional Medical Center LLC or its associated clinics and whose Sensitive

Information was wrongfully accessed, copied, and transferred in the months on or about April 2014 and June 2014.

55. Excluded from the Classes and Subclasses are (1) any judge presiding over this action and members of their families; (ii) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Classes; and (iv) the legal representatives, successors, or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of the data stored by Defendants.

56. **Defendant Class:** CHS, CHSPSC, and all of its subsidiaries and affiliate hospitals, medical centers and clinics, as represented by the eight individually named New Mexico hospital and medical center and medical clinic defendants in this lawsuit.

57. **Numerosity.** Members of the Classes are so numerous that their individual joinder herein is impracticable. Although the exact number of Class members and their addresses are unknown to Plaintiff, they are readily ascertainable from Defendants' records. Upon information and belief, there are thousands of class members in the national and state-wide classes. Class members may be notified of the pendency of this action by mail and/or electronic mail, and supplemented (if deemed necessary or appropriate by the Court) by published notice.

58. **Typicality**. Plaintiffs' claims are typical of the Classes because Plaintiffs and the Classes sustained damages as a result of Defendants' uniform wrongful conduct during transactions with Plaintiffs and Classes.

59. **Adequacy**. Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the members of the Class they seek to represent. Plaintiffs have retained counsel competent and experienced in class action litigation, and

Plaintiffs intend to prosecute this action vigorously. The interests of members of the Classes will be treated fairly and will be adequately protected by Plaintiffs and their counsel.

60. **Predominance and Superiority:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. The damages suffered by the individual members of the Classes will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendants' misconduct. Even if members of the Classes could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Finally, economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

61. **Commonality:** Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting only individual members. These include, but are not limited to:

a. Whether Defendants were negligent in collecting, storing, and protecting Plaintiffs' and the Class Members' Sensitive Information;

b. Whether Defendants were wanton in collecting, storing, and protecting Plaintiffs' and the Class Members' Sensitive Information;

c. Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' Sensitive Information;

d. Whether Defendants breached their duty to exercise reasonable care in handling Plaintiffs' and Class Members' Sensitive Information by storing that information in the manner alleged herein;

e. Whether Defendants notified Plaintiffs and the Classes of the data breach within a reasonable amount of time;

f. Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiffs and the Class members, on the other;

g. Whether Plaintiffs and the Classes identity was stolen, and whether they are at an increased risk of identity theft or other malfeasance as a result of Defendants' failure to protect their Sensitive Information;

h. Whether Defendants stored Plaintiffs' and the Class Members' Sensitive Information in a reasonable manner under industry standards;

i. Whether protecting Plaintiffs' and the Class Members' Sensitive Information was a service promised by Defendants;

j. Whether Defendants unlawfully retained payment from Plaintiffs and the Class Members because of Defendants' failure to fulfill their agreement to protect their Sensitive Information;

k. Whether and to what extent Plaintiffs and the Class Members have sustained damages.

l. Whether Defendants were unjustly enriched;

m. Whether Defendants breached their duty of confidentiality to Plaintiffs and the Class members;

n. Whether Defendants violated statutory law in their handling of Plaintiffs' and the Class Members' Sensitive Information.

62. Plaintiff reserves the right to revise Class definitions and questions based upon facts learned in discovery.

VII. CAUSES OF ACTION

Count 1 – Unjust Enrichment

63. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

64. Defendants received payment from Plaintiffs and the Class members to perform services that included protecting their Sensitive Information.

65. Defendants did not protect Plaintiffs' and the Class Members' Sensitive information, but retained Plaintiffs' payments.

66. Defendants have knowledge of said benefit.

67. Defendants have been unjustly enriched and it would be inequitable and unjust for Defendants to retain Plaintiffs' and the Class Members' payments.

68. As a result, Plaintiffs have been proximately harmed and/or injured.

69. WHEREFORE, Plaintiffs demand judgment against Defendants concurrently, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs and the Class members for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 2—Money Had and Received

70. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

71. Defendants have received payment from Plaintiffs and the Class members to perform services that included protecting Plaintiffs' and the Class Members' Sensitive Information.

72. Defendants did not protect Plaintiffs' and the Class Members' Sensitive Information, but retained their payments.

73. The law creates an implied promise by Defendants to refund such payments to Plaintiffs and the Class members.

74. Defendants have breached said implied promise.

75. Defendants' breach has proximately caused Plaintiffs and the Class members to suffer harm and damages.

76. WHEREFORE, Plaintiffs demand judgment against Defendants concurrently, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs and the Class members for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 3—Breach of Contract (Express and Implied)

77. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

78. Plaintiffs and the Class members paid money to Defendants in exchange for hospital's services, which included promises to protect Plaintiffs' and the Class Members' health information and Sensitive Information.

79. In their written services contract, Defendants promised Plaintiffs and the Class members that Defendants would only disclose health information when required to do so by

federal or state law. Defendants further promised that they would protect Plaintiffs' and the Class Members' Sensitive Information.

80. Defendants promised to comply with all HIPAA standards and to make sure that Plaintiffs' and the Class Members' health information and Sensitive Information were protected.

81. Defendants' promises to comply with all HIPAA standards and to make sure that Plaintiffs' and the Class Members' health information and Sensitive Information were protected created an express contract.

82. To the extent that it was not expressed, an implied contract was created whereby Defendants promised to safeguard Plaintiffs' and the Class Members' health information and Sensitive Information from being accessed, copied, and transferred by unauthorized third parties.

83. Under the implied contract, Defendants were further obligated to provide Plaintiffs and the Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

84. Defendants did not safeguard Plaintiffs' and the Class Members' health information and Sensitive Information and, therefore, breached their contract with Plaintiffs and the Class members.

85. Defendants allowed unauthorized third parties to access, copy, and transfer Plaintiffs' and the Class Members' health information and Sensitive Information and, therefore, breached their contract with Plaintiffs and the Class members.

86. Furthermore, Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs and the Class members that were of a diminished value.

87. As a result, Plaintiffs and the Class members have been harmed and/or injured.

88. WHEREFORE, Plaintiffs demand judgment against Defendants concurrently, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 4—Negligence

89. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

90. Defendants requested and came into possession of Plaintiffs' and the Class Members' Sensitive Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being accessed. Defendants' duty arose from the industry standards discussed above and their relationship with Plaintiffs and the Class members.

91. Defendants had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and the Class Members' Sensitive Information. The breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class and Subclasses were reasonably foreseeable, particularly in light of Defendants' inadequate data security system and failure to adequately encrypt the data.

92. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's Sensitive Information within Defendants' control.

93. Defendants, through their actions and/or omissions, breached their duty to Plaintiffs and the Class members by failing to have procedures in place to detect and prevent access to Plaintiffs' and the Class Members' Sensitive Information by unauthorized persons.

94. But for Defendants' breach of their duties, Plaintiffs' and the Class Members' Sensitive Information would not have been compromised.

95. Plaintiffs' and the Class Members' Sensitive Information was stolen and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such information by adopting, implementing, and maintaining appropriate security measures and encryption.

96. Defendants knew, were substantially aware, should have known, or acted in reckless disregard of the fact that Plaintiffs and the Class members would be harmed if Defendants did not safeguard and protect Plaintiffs' and the Class Members' Sensitive Information. As a result, Plaintiffs and the Class members have been harmed and/or injured.

97. WHEREFORE, Plaintiffs demand judgment against Defendants concurrently, for compensatory and punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs and the Class members for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 5—Negligence Per Se

98. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

99. Defendants' violation of HIPAA resulted in an injury to Plaintiffs and the Class members.

100. Plaintiffs and the Class members fall within the class of persons HIPAA was intended to protect.

101. The harms Defendants caused to Plaintiffs and the Class members are injuries that result from the type of behavior that HIPAA was intended to protect against.

102. As a result, Plaintiffs and the Class members have been harmed and/or injured.

103. WHEREFORE, Plaintiffs demand judgment against Defendants concurrently, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs and the Class members for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 6—Breach of Confidence / Wrongful Disclosure of Confidential Communication

104. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

105. A relationship of trust and confidence exists between Plaintiffs and the Class members and Defendants as their health care providers.

106. Defendants owed a duty of confidence to Plaintiffs and the Class members.

107. Defendants were entrusted with Plaintiffs' and the Class Members' confidential information.

108. Defendants breached their duty to Plaintiffs and the Class members by failing to safeguard and protect such information from disclosure to unauthorized persons.

109. Plaintiffs and the Class members suffered damages as a result of Defendants' breach of their duty of confidence.

110. Wherefore, Plaintiffs demand judgment against Defendants concurrently, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs and the Class members for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 7 – Violation of the NM Unfair Trade Practices Act, NMSA 57-12-1 et seq.

111. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

112. Defendants violated the Unfair Trade Practices Act in connection with the sale of services or in the extension of credit to Plaintiffs and the Class members in their regular course of business and commerce that tended to or did deceive Plaintiffs and the Class members, specifically, a) representing that goods or services were of a specific quality when they were not; b) stating that the transactions made with Plaintiffs and the Class members involved certain rights, remedies or obligations that the transactions did not involve; and, c) failing to deliver the quality of services contracted for. NMSA 57-12-2 (D)(7), (15), & (17).

113. Defendants knowingly made the false or misleading statements or representations listed above to Plaintiffs and the Class members.

114. Pursuant to NMSA 57-12-10, in any class action filed under the Unfair Trade Practices Act, the named Plaintiffs as well as the Class members may recover actual monetary damages.

115. Wherefore, Plaintiffs demand judgment against Defendants concurrently, for compensatory and/or punitive damages, the sum to be determined by a jury, and injunctive relief, which will fairly and adequately compensate Plaintiffs and the Class members for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count 8 – Willful Violation of the Fair Credit Reporting Act

116. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as if fully set out herein.

117. The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

118. FCRA specifically protects medical information, restricting its dissemination to limited instances. See, e.g., 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

119. Defendants are a Consumer Reporting Agency as defined under FCRA because on a cooperative nonprofit basis and/or for monetary fees, Defendants regularly engage, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

120. By collecting, gathering and storing information bearing on consumers' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, Defendants create "consumer reports" on their patients, which they transmit to medical service providers affiliated with Defendants to use for the purpose of establishing patient's eligibility for credit for medical treatments and services, rendering each Defendants a "consumer reporting agency" under the FCRA.

121. As a Consumer Reporting Agency, Defendants were (and continue to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiffs' and Class Members' Personal Identifying Information and Personal Health Information, "PII/PHI") in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. Defendants, however, violated FCRA by failing to adopt and

maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of Plaintiffs' and its wrongful dissemination into the public domain.

122. Plaintiffs' PII/PHI, in whole or in part, constitutes medical information as defined by FCRA. Defendants violated FCRA by failing to specifically protect and limit the dissemination of Plaintiffs' PII/PHI into the public domain.

123. As a direct and/or proximate result of Defendants' willful and/or reckless violations of FCRA, as described above, Plaintiffs' PII/PHI was stolen and/or made accessible to unauthorized third parties in the public domain.

124. As a direct and/or proximate result of Defendants' willful and/or reckless violations of FCRA, as described above, Plaintiffs were (and continue to be) damaged in the form of stolen identity, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

125. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) out-of-pocket expenses incurred as a result of the identity theft and to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

126. WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which

will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

Count Nine-- Negligent Violation of the Fair Credit Reporting Act

127. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as fully set out herein.

128. In the alternative, and as described above, Defendants negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiffs' PII/PHI for the permissible purposes outlined by FCRA which, in turn, directly and/or proximately resulted in the theft and dissemination of Plaintiffs' PII/PHI into the public domain.

129.

It was reasonably foreseeable that Defendants' failure to implement and maintain procedures to protect and secure Plaintiffs' PII/PHI would result in an unauthorized third party gaining access to Plaintiffs' PII/PHI for no permissible purpose under FCRA.

130. As a direct and/or proximate result of Defendants' negligent violations of FCRA, as described above, Plaintiffs' PII/PHI was stolen and/or made accessible to unauthorized third parties in the public domain.

131. As a direct and/or proximate result of Defendants' negligent violations of FCRA, as described above, Plaintiffs were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

132. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) out-of-pocket expenses incurred to pay for the stolen data and to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the

Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

VIII. RELIEF REQUESTED

133. Based on the above allegations, Plaintiffs respectfully ask the Court to:

a. Certify this case as a class action on behalf of the Class and Subclasses as defined above, and appoint named Plaintiffs as class representatives and undersigned counsel as lead counsel;

b. Find that Defendants are liable under all legal claims asserted herein for their failure to safeguard Plaintiffs' and the Class Members' Sensitive Information;

c. Award injunctive and other equitable relief as is necessary to protect the interests of the Classes, including: (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Defendants to protect all data collected through the course of its business in accordance with HIPAA and industry standards, (iii) consumer credit protection and monitoring services for Plaintiffs and the Class members; and (iv) consumer credit insurance to provide coverage for

unauthorized use of Plaintiffs' and the Class Members' personal information, medical information, and financial information;

d. Award damages, including statutory damages where applicable and punitive damages, to Plaintiffs and the Classes in an amount to be determined at trial;

e. Award restitution for any identity theft, including, but not limited to payment of any other costs, including attorneys' fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of Defendants' actions;

f. Award restitution in an amount to be determined by an accounting of the difference between the price Plaintiffs and the Classes paid in reliance upon Defendants' duty/promise to secure their Sensitive Information, and the actual services—devoid of proper protection mechanisms—rendered by Defendants;

g. Award Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

h. Award Plaintiffs and the Classes pre and post-judgment interest to the maximum extent allowable by law; and

i. Award such other and further legal or equitable relief as equity and justice may require.

IX. JURY DEMAND

134. Plaintiffs demand a jury trial on all issues in this action.

Date: December 5, 2014

Respectfully submitted:

Branch Law Firm

By: */s/ Mary Lou Boelcke*

Turner W. Branch
Margaret Moses Branch
Mary Lou Boelcke
2025 Rio Grande Blvd. NW
Albuquerque, NM 87104
Phone (505) 243-3500
Fax (505) 243-3534

Slack & Davis LLP
Michael Slack
Paula Knippa
2705 Bee Cave Rd., Ste. 220
Austin, TX 78746
Phone (512) 795-8686

CERTIFICATE OF SERVICE

I certify that a true and correct copy of the foregoing was served via the Court's CM/ECF system on this 5th day of December, 2014, to the following:

Paul Karlsgodt
pkarlsgodt@bakerlaw.com

David A. Carney
dcarney@bakerlaw.com

Theodore J. Kobus
tkobus@bakerlaw.com
Counsel for Community Health Systems Professional Services, Corporation

Michael J. Dekleva
mjd@madisonlaw.com
Counsel for Alta Vista Regional Hospital, Carlsbad Medical Center, Eastern New Mexico Medical Center, Mimbres Memorail Hospital, Mountainveiw Regional Medical Center and Lea Regional Medical Center

By: */s/ Mary Lou Boelcke*